計算量理論における記述集合論的問題について(数学基礎論とその応用)

AUTHOR(S):

田中, 尚夫

CITATION:

田中, 尚夫. 計算量理論における記述集合論的問題について(数学基礎論とその応用). 数理解析研究所講究録 1991, 772: 126-137

ISSUE DATE:

1991-12

URL:

http://hdl.handle.net/2433/82377

数理解析研究所講究録
772巻 1991年 126-137

計算量理論における記述集合論的問題について

法政大工　田中尚夫 （ Hisao Tanaka ）

記述集合論で起った若干の問題を計算量理論へもち込む．ここでは次の三つの話題について述べる．

1）　$\{X \subseteq \Sigma^* : \mathbf{P}[X] \neq \mathbf{NP}[X]\}$　のような いくつかの特別なクラスの Arithmetical (or Borel) Hierarchy における位置の決定：このようなクラスが proper Π^0_2 クラスであることが示される．

2）　計算量理論における Uniformization Problem の考察：　一意化 Unif($\mathbf{P}$[A]), Unif($\mathbf{NP}$[A]), 及び Unif($\mathbf{coNP}$[A]) が成り立つような oracle A の存在は自明である．　よって，そうでない oracle A の存在が問題である．　ここでは，a) 或 $S \in \mathbf{P}$[A] に対して，その典型的な一意化 U_S が $\mathbf{NP}$[A] に属さないような oracle A が存在すること；　b) Unif($\mathbf{coNP}$[A]) が成立しないような oracle A が存在すること；などを示す．

3）　Reduction Principle　及び　Separation Principle の計算量理論におけるアナロジー：　a)　$\mathbf{NEXT}$ に対して Reduction Principle が成立すること；b) $\mathbf{NP}$[A] に属する二つの集合で $\mathbf{P}$[A]-inseparable なものが存在するような oracle A があること；などを示す．

また，いくつかの未解決問題を述べる．

§ 1 . 準備事項. 計算量理論と記述集合論における標準的な記号を用いる. $\Sigma = \{0, 1\}$ はアルファベット, Σ^* は Σ 上の語全体の集合で空語 λ を含むとする. u, v, w, x, ... は語を表し, A, B, ..., X, Y, ... は語の集合を表す. 次のような, 語の線形順序 ($<$) を用いる:

$$\lambda, 0, 1, 00, 01, 10, 11, 000, 001, \ldots$$

語 x の長さを $|x|$ で表す. そのとき, $|x| \leq n$ ならば $x < 0^{n+1}$ である. π は $\Sigma^* \times \Sigma^* \to \Sigma^*$ なる多項式時間計算可能な全単射対関数, π_0 と π_1 はその多項式時間計算可能な逆関数である:

$$\pi(\pi_0(z), \pi_1(z)) = z \quad \text{for any } z \in \Sigma^*.$$

$\pi(x,y)$ の代わりに $\langle x,y \rangle$ と書く. 従って, $\Sigma^* \times \Sigma^*$ の部分集合は Σ^* の部分集合と考えてよい.

$\wp(\Sigma^*)$ は Σ^* の全ての部分集合の集合である. 多くの場合 ('開集合' というような慣用を除いて) $\wp(\Sigma^*)$ の部分集合をクラスと呼ぶ. $\wp(\Sigma^*)$ はカントル空間である.

よく知られた **P**, **P**[A], **NP**, **NP**[A], etc のようなクラスについては, 文献 [BDG 88], [BDG 90] などを参照されたい.

§ 1 . 特別ないくつかのクラスの分類. 次に述べるクラスの, 算術的階層におけるレベルを決定する:

$$\mathbf{E}_1 = \{ X \subseteq \Sigma^* : \mathbf{P}[X] \neq \mathbf{NP}[X] \},$$

$$\mathbf{E}_2 = \{ X : \mathbf{coNP}[X] \neq \mathbf{NP}[X] \},$$

$$E_3 = \{ X : DEXT[X] \neq NEXT[X] \},$$

$$E_4 = \{ X : coNEXT[X] \neq NEXT[X] \},$$

$$E_5 = \{ X : P[X] \neq PH[X] \},$$

$$E_6 = \{ X : NP[X] \neq PH[X] \},$$

$$E_7 = \{ X : NP[X] \neq PSPACE[X] \},$$

$$E_8 = \{ X : NP[X] \neq EXPTIME[X] \},$$

$$E_9 = \{ X : PH[X] \neq PSPACE[X] \},$$

$$E_{10} = \{ X : PSPACE[X] \neq EXPTIME[X] \}.$$

とおく．これらの間の包含関係は次のようである（$\subset$ は真の包含関係を表す）：

$$E_2 = E_6 \subset E_1 = E_5, \quad E_4 \subset E_3 \subset E_1 \neq E_7,$$

$$E_6, E_9 \subseteq E_7 \subseteq E_8, \quad E_6 \subset E_8, \quad E_{10} \subseteq E_8.$$

ここで，$\subseteq$ が $\subset$ であるかどうかを決定することも一つの問題である．

定理 1．各 E_k は Π^0_2 であるが，Σ^0_2 でない．実際 Borel 階層における F_σ でさえない．□

この定理は次の一般的定理の系として得られる．

定理 2．$B[X]$, $C[X]$ が X-recursively presentable なクラス [1] で，$E = \{ X : B[X] \neq C[X] \}$ とし，次の条件が満たされているとする：

(a) (a1) $B[X] \subseteq C[X]$ for all X, 又は (a2) $B[X] = coC[X]$ for all X,

(b) (b1) P-m-還元性について，又は (b2) 線形還元性について $C[X]$-完全な集合 $H(X)$ が存在する，

(c) $B[X]$ は (c1) 多項式的に閉じている，か又は (c2) 線形的に閉じている [2]，

(d)　$\mathbf{E}$ は meager でもなく，また 全空間 $\wp(\Sigma^*)$ でもない，

(e)　$\mathbf{E}$ は tail set [3] である．

以上の条件の下に，$\mathbf{E}$ は proper Π^0_2 クラスである．　実際，それは F_σ でさえない．　ただし，(b1) と (c1) が組合わされ，(b2) と (c2) が組合わされる．

（注）　1) [Sch 82] または [BDG 88] を参照．

2) f(y) が多項式時間計算可能又は線形時間計算可能であり，$L \in \mathbf{B}[X]$ であれば，$f^{-1}(L) \in \mathbf{B}[X]$ であること．

3) [Ox 71] を参照．

証明の概略．　定理における条件 (b),(c) をもちいて，$X \in \mathbf{E} \Leftrightarrow H(X) \notin \mathbf{B}[X]$ が示される．　$\mathbf{B}[X]$ が X-recursively presentable であるから，右辺は Π^0_2 形で表せる．　そこで，$\mathbf{E}$ が F_σ であるとしょう．　補集合 $\neg\mathbf{E}$ は空でない tail set であり，従ってそれは dense である．　$\mathbf{E}$ は meager な F_σ 集合だから 任意の dense set と交わる．　よって特に，$\mathbf{E} \cap \neg\mathbf{E} \neq \phi$．これは不合理．　ゆえに，$\mathbf{E}$ は F_σ でなく，従って勿論 Σ^0_2 でない．□

<u>定理１の証明</u>：　各 $\mathbf{E}_k$ は定理２の諸条件を満足する．　その証明には，[BG 81], [Po 85] などの結果が利用される．□

上記の諸クラス以外にも類似なクラスが色々ある．　例えば $\mathbf{E} = \{ X : \mathbf{P}[X] \neq \mathbf{BPP}[X] \}$ を考えよう．　$\mathbf{BPP}[X]$ の定義に従って直接的に評価することにより，$\mathbf{E}$ が Σ^0_3 であることが示される．　しかし，それが Π^0_3 であるか否かまだわからない．　上と同様な論法で F_σ でないことはわかる．　その正確な位置を決定することは未解決である．

§ 2. Uniformization の問題. Uniformization と separation の問題は記述集合論の中心的問題である. これは階層に関連するので, 計算量理論における複雑さ(計算量)と関係づけることができる. $S \subseteq \Sigma^*$ が与えられたとき,

(1) $U \subseteq S$,

(2) $\exists y (\langle x,y \rangle \in S) \Rightarrow \exists! y (\langle x,y \rangle \in U)$

をみたす U は S を一意化する(uniformize)といい, U を S の unifomizator と呼ぶ. U は定義域 $D_S = \{ x : \langle x,y \rangle \in S \}$ で定義された或部分関数のグラフである. さて, 問題は U を S からどのようにして求めるかである. 即ち, S が或計算量クラスに属するとき, どんなクラスの uniformizator U を求められるかという問題である. 記述集合論において, これに関する最も有名な結果は Novikov-Kondo-Addison の定理であろう: Π^1_1 集合は Π^1_1 集合によって一意化できる. (勿論この場合は例えば $N^N \times N^N$ の部分集合について言っている. [Mo 80])

定義. Unif(C;K) は次の主張を表す: 各 $S \in C$ に対して, (1) 及び (2) を満たす $U \in K$ が存在する. 従って次の (3) が成立する:

(3) $\exists y (\langle x,y \rangle \in S) \Leftrightarrow \exists! y (\langle x,y \rangle \in U) \Leftrightarrow \exists y (\langle x,y \rangle \in U)$.

また, Unif(C;C) を Unif(C) と略記する. □

補題3. C が conjunction 演算, 補集合演算, 及び有界全称作用素 $\forall z < y$ の下で閉じているならば, Unif(C) が成立つ.

証明. $S \in C$ とする. U_S を次式で定義する:

(4) $\langle x,y \rangle \in U_S \Leftrightarrow \langle x,y \rangle \in S \wedge \forall z (z < y \Rightarrow \langle x,z \rangle \notin S)$.

U_S は明らかに S の uniformizator であり, C に属する. □

今後のために，U_S を S の底曲線と呼ぶことにする．

系４．　Unif(**DEXT**) が成り立つ．

証明．　**DEXT** は 補題３ の条件を満たす．　$\#\{ z : z < y \} \fallingdotseq 2^{|y|+1}$ に注意．□

ところで，　$\forall z < y [\ldots]$　は　$\forall z [|z| \leqq |y| \Rightarrow (z < y \Rightarrow \ldots)]$ と表せるから，もし　**NP = coNP**　（ または　**P = NP** ）ならば，Unif(**NP**)（ または　Unif(**P**) ）が成立つ．　よって，[BGS 75] により

命題５．　Unif(**NP**[A]), Unif(**coNP**[A]), 及び　Unif(**P**[A]) が成り立つような oracle A が存在する．□

次に，部分関数　$f : \Sigma^* \to \Sigma^*$　が多項式時間計算可能とは，その定義域 Dom(f) が **P** に属し，すべての　$x \in Dom(f)$ に対し値 f(x) が多項式時間限定 Turing machine によって計算できること．　そのとき次の問が起こる：

問題１．　**P** に属する集合は必ず多項式時間計算可能関数によって一意化できるか ？

これはなかなか解決が困難であるように思われる．　しかし，**P** に或制限を付け加えるならば，肯定的に解ける：

命題６．　$\log\mathbf{P} = \{ Q :$ For some $c>0$ and some $S \in \mathbf{P}$, $\langle x,y\rangle \in Q \Leftrightarrow |y| \leqq c \cdot \log|x| \wedge \langle x,y\rangle \in S \}$　とする．　このとき，$\log\mathbf{P}$ に属する集合は多項式時間計算可能関数で一意化できる．

証明．　$\#\{y : |y| \leqq c \cdot \log|x| \} \leqq 2|x|^c$　であるから，$Q \in \log\mathbf{P}$ ならば，$D_Q = \{ x : \exists y (\langle x,y\rangle \in Q)\}$ は **P** に属する．　これより，Q の底曲線

U_Q が多項式時間計算可能関数であることがわかる． □

これに対し，

命題７． 次のような recursive oracle A が存在する： $\mathbf{P}[A]$ に属する或集合 S があって，S のどの unformizator も A-多項式時間計算可能関数では一意化できない．

証明． $\mathbf{NP}[A]$-完全な集合 K(A) が $\mathbf{P}[A]$ に属さないような recursive oracle A をとる． K(A) は，或 $R \in \mathbf{P}[A]$ と或多項式 p(n) について

$$x \in K(A) \Leftrightarrow \exists y\,(\,|y| \leqq p(|x|) \wedge \langle x,y\rangle \in R\,)$$

と表せるから，S として $S = \{\,\langle x,y\rangle : |y| \leqq p(|x|) \wedge \langle x,y\rangle \in R\,\}$ をとればよい．□

これと対比して，次の問いは少し難しいように思える：

問題２． Unif($\mathbf{P}[A]$) が成り立たないような oracle A が存在するか ？

部分的解答として，

定理８． 次のような recursive oracle A が存在する： 或 $S \in \mathbf{P}[A]$ があって，S の底曲線 U_S は $\mathbf{NP}[A]$ に属さない．□

S が $\mathbf{NP}[A]$ の集合でよいなら，定理８の証明は容易である： そのために，$\mathbf{NP}[A] - \mathbf{coNP}[A] \neq \phi$ なる recursive oracle A をとり，E をそのクラスの一つの集合とせよ． $S = \{\,\langle x,y\rangle : (\,x \in E \wedge y = 0\,) \vee y = 1\,\}$ とすれば S の底曲線 U_S は $\mathbf{NP}[A]$ に属さない．（この論法は，類似な問題についての H. Enderton との会話に基づく．）

定理８の証明． $X \subseteq \Sigma^*$ に対し，

$$L(A) = \{ \langle x,y \rangle : \exists z (z \prec y \wedge \langle x,y \rangle \in X)\}$$

とおく． oracle A を段階で定義し，[BGS 75] におけるように

(5) $L(A) \in \mathbf{coNP}[A]$

が成り立つようにする． A(s) は段階 s より前の段階までに A へ取り込まれた語全体の集合で， $A(0) = \phi$ として出発する． また，s に応じて自然数 n_s を定義する． $n_0 = 0$ とする． 更に，$\ell(n) = |\langle 1^n, 0^{n+1} \rangle|$ とおく． $\ell(n)$ は n の一次関数であるとしてよい．

段階 $s \geqq 0$． n を $n > n_s$ かつ $p_s(\ell(n)) < 2^n$ なる最小の数とする． 但し $p_s(n)$ は s 番目の非決定性多項式時間限定 oracle Turing machine $NP_s^{\sim}$ の時間限定関数である． 先ず， $B(s) = A(s) \cup \{ \langle 1^n, 0^{n+1} \rangle \}$ とし，入力 $\langle 1^n, 0^{n+1} \rangle$ 上で $NP_s^{B(s)}$ を走らせる． もしそれが受理すれば，受理計算過程を一つ選び（確定のため各分岐の最初を選ぶ）その計算中 oracle に質問されない $\langle 1^n, u \rangle$ なる形の語を一つとり B(s) へ加えて A(s+1) を作る（かかる語 u は存在する；確定のためそれが $\prec$-最小となるものを選ぶ）． もし受理しなければ，何もしない： 即ち $A(s+1) = B(s)$ とする． $n_{s+1} = 2^n$ とおく． 各々の段階 s で A へ加えられた語は s より前の段階での計算に影響を与えない．

A はすべての A(s) たちの和集合であると定義する． A は明らかに recursive set である． 任意の s について

NP_s^A が $\langle 1^n, 0^{n+1} \rangle$ を受理する $\Leftrightarrow$ $NP_s^{B(s)}$ が $\langle 1^n, 0^{n+1} \rangle$ を受理する

$\Leftrightarrow \exists u (|u| = n \wedge \langle 1^n, 0^{n+1} \rangle \in A)$

$\Leftrightarrow \exists u (u \prec y \wedge \langle 1^n, 0^{n+1} \rangle \in A) \Leftrightarrow \langle 1^n, 0^{n+1} \rangle \in L(A)$

$\Leftrightarrow \quad \langle 1^n, 0^{n+1} \rangle \notin \neg L(A)$.

よって，(5) が成り立つ． そこで，A の底曲線 U_A を考える：

$$\langle x,y \rangle \in U_A \Leftrightarrow \langle x,y \rangle \in A \wedge \forall z (z < y \Rightarrow \langle x,z \rangle \notin A).$$

L(A) は U_A より上にある点 $\langle x,y \rangle$ の集合である． 今，R を U_A 以下にある点全体の集合としよう：

$$\langle x,y \rangle \in R \Leftrightarrow \exists z (y \leqq z \wedge \langle x,z \rangle \in U_A).$$

もし $\langle x,z \rangle \in U_A$ ならば $|z| \leqq |x| + 1$ であるから，

(6) $\langle x,y \rangle \in R \Leftrightarrow \exists z [|z| \leqq |x| + 1 \wedge (y \leqq z \wedge \langle x,z \rangle \in U_A)]$

となる． そこで，$U_A \in \mathbf{NP}[A]$ と仮定しよう． すると (6) により $R \in \mathbf{NP}[A]$ となる． 他方，作り方から A の domain $D_A \in \mathbf{P}[A]$ であり，従って $L(A) = D_A \times \Sigma^* - R \in \mathbf{coNP}[A]$ となってしまう． これは (5) と矛盾する． よって， $U_A \notin \mathbf{NP}[A]$ でなければならない． $A \in \mathbf{P}[A]$ であるから，$S = A$ ととって定理は証明された．□

この定理において，当該の uniformizator は特別なものである． S は $\mathbf{P}[A]$ に属する或集合で一意化出来るかも知れない． 事実，定理の証明で用いられた S (= A) は $\mathbf{P}[A]$ に属する集合で一意化される． 我々は S のどんな unifomizator も $\mathbf{P}[A]$ には属さないような A と S を求めたいのである． これが問題２である．

では，$\mathbf{P}[A]$ に属する集合はどんなクラスの集合によって一意化できるのだろうか ？

命題９． $\mathrm{Unif}(\mathbf{P};\mathbf{coNP})$ が成り立つ．

証明． $S \in \mathbf{P}$ とする． S の底曲線 U_S は次のように表される：

$\langle x,y\rangle \in U_S \Leftrightarrow \langle x,y\rangle \in S \wedge \forall z\,[\,|z| \leqq |y| \Rightarrow (\,z < y \Rightarrow \langle x,z\rangle \notin S)]$.

よって，$U_S \in \mathbf{coNP}$ である．□

問題１′（問題１の弱い形） Unif(P) が成立つか ？

§３． 還元原理と分離原理．

C を一つの計算量クラスとする．

$$\mathrm{Red}(\mathbf{C}) \Leftrightarrow \forall X,Y\in\mathbf{C}\ \exists X_1,Y_1\in\mathbf{C}\ [\,X_1\subseteq X \wedge Y_1\subseteq Y \wedge X_1\cup Y_1 = X\cup Y \wedge X_1\cap Y_1 = \phi\,],$$

$$\mathrm{Sep}(\mathbf{C}) \Leftrightarrow \forall X,Y\in\mathbf{C}\ [\,X\cap Y=\phi \Rightarrow \exists Z\in\mathbf{C}\cap\mathbf{coC}\ (\,X\subseteq Z \wedge Z\cap Y=\phi\,)]$$

とおく． そのとき，

C に対する還元原理とは： Red(C) が成立すること，

C に対する分離原理とは： Sep(C) が成立すること．

非常に広い範囲のクラスたちに対して

(7) $\mathrm{Unif}(\mathbf{C}) \Rightarrow \mathrm{Red}(\mathbf{C}) \Rightarrow \mathrm{Sep}(\mathbf{coC})$

が成り立つことが知られている（[Mo 80]）．

$$X \in \mathbf{NEXT} \Leftrightarrow \exists a>0\ \exists R\in\mathbf{P}\ \forall x\ [\,x\in X \Leftrightarrow \exists y(\,|y|\leqq 2^{a|x|} \wedge \langle x,y\rangle\in R\,)]$$

であることを利用すれば，次の結果が得られる：

命題１０． Red(NEXT) が成立する． 従って Sep(coNEXT) が成り立つ． □

問題３． Red(NP) は成立するか ？

次に，$\mathbf{C}$ と $\mathbf{E}$ を $\mathbf{E} \subset \mathbf{C}$ なる計算量クラスとし，B,C は $\in \mathbf{C}$ であって互に素な集合とする． B と C が $\mathbf{E}$-分離可能 とは，$R \in \mathbf{E}$, $B \subseteq R$, $R \cap C = \phi$ なる集合 R が存在することである． そうでないとき，B と C は $\mathbf{E}$-分離不可能 であるという． このとき，

定理１１． 次の条件を満たす recursive oracle A が存在する： $\mathbf{NP}[A]$ は $\mathbf{P}[A]$-分離不可能な disjoint sets をもつ．

証明の概略． $K_0(A) = \{ x : \exists y (0y \in A \wedge |0y| = |x|)\}$, $K_1(A) = \{ x : \exists y (1y \in A \wedge |1y| = |x|)\}$ とおく． この二つの集合が互に素で，$\mathbf{P}[A]$ に属する集合では分離できないように，段階で A を定義する．□

これは，自然数の recursively enumerable disjoint sets で recursively inseparable なものが存在する，という古典的定理に対応するものである．

この定理は，このままでは $\neg$Sep($\mathbf{NP}[A]$) を含意しない． なぜなら，$K_0(A)$ と $K_1(A)$ が $\mathbf{NP}[A] \cap \mathbf{coNP}[A] - \mathbf{P}[A]$ に属する集合で分離できるかも知れないからである． しかし，[BGS 75] の Theorem 6 の証明を修正することによって次の結果が得られる：

定理１２． Sep($\mathbf{NP}[A]$) が成立しないような recursive oracle A が存在する． □

この結果と (7) とを組合わせることにより，次の定理を得る：

定理１３． Unif($\mathbf{coNP}[A]$) が成立しないような recursive oracle A が存在する． □

なお，定理１１に対応して次の結果も得られる：

定理１４．　次の条件を満たす recursive oracle A が存在する：**NEXT**[A] は **DEXT**[A]-分離不可能な disjoint sets をもつ．　□

問題４．　Sep(**NEXT**[A]) が成立しないような oracle A が存在するか ？

文献

[BGS 75] Baker,T., Gill,J., and Solovay,R., Relativizations of the P = ?NP question, SIAM J. Comput., 4 (1975), 431-442.

[BDG 88] Balcázar,J.L.,Díaz,J., and Gabarró,J., Structural Complexity I, Springer-Verlag, Berlin etc. (1988).

[BDG 90] --- , --- --- II, --- (1990).

[BG 81] Bennett,C.H., Gill,J., Relative to a random oracle A, $P^A \neq NP^A \neq coNP^A$ with probability 1, SIAM J. Comput., 10 (1981), 96-113.

[Mo 80] Moschovakis,Y.N., Descriptive set theory, North-Holland Publ. Co., Amsterdam etc. (1980).

[Ox 71] Oxtoby,J.C., Measure and Category, Spriger-Verlag, New York etc., (1971)

[Po 86] Poizat,B., Q = NQ ?, J. Symbolic Logic, 51 (1986), 22-32.

[Sch 82] Schoning,U., A uniform approach to obtain diagonal sets in complexity classes, Theor. Comput. Sci., 18 (1982), 95-103.